Security System

The invention relates to a security system for identity and authorization checking in a protected communication environment.

BACKGROUND OF THE INVENTION

The identity and authorization checking is performed in a protected communication environment using, as a rule, personal identifiers in combination with a memory card or chip card. A user of an automatic teller machine, for instance, is required to first insert a bank card and then enter the user's personal identification number. Experience has shown that identity and authorization checks of this kind are not sufficient to avoid any abuse. It is not only awkward to enter the personal identification number, but this number is also relatively easy to spy out.

Identity and authorization checks which are considered to be very secure are those performed by means of a fingerprint sensor. High-resolution sensors operating in accordance with the principle of a capacitive matrix have been disclosed, which derive unique and unmistakable characteristics from a fingerprint and, after a highly effective data reduction, make such characteristics available as a characteristic data set. This characteristic data set may, in one application, be stored as an access and authorization condition. In such a system the entry of a personal identification code is not required. However, it can not be excluded in principle that the characteristic data set provided by the fingerprint sensor is intercepted or spied out while on its transmission path.

SUMMARY OF THE INVENTION

The invention creates a security system which provides very high protection while doing without the user having to enter a personal identification code. According to the

invention, the security system comprises a chip card reader in the format of a PC card which has personal data stored thereon. Coupled to the chip card reader is a fingerprint sensor. A validation means validates the personal information read from the chip card depending on data provided by the fingerprint sensor. For a positive outcome of an identity and authorization check, both the chip card with the personal data needs to be available and also the characteristic data set provided by the fingerprint sensor needs to be correctly related to the personal data stored on the chip card.

The security system in accordance with the invention allows to establish a highly secure control of the communication between a local data processing apparatus and a network. According to a first approach, in which the fingerprint sensor is integrated in the chip card reader, the security system comprises an interface for connection to the network. The interface involved may be a conventional network media adapter, a modem, or an IR interface. The local data processing apparatus and the network can communicate only via the security system. By providing such a security system it can be ensured that only authorized users are permitted to access the network. Provision can further be made that all messages transmitted in one or in both directions are signed by the characteristic data set provided by the fingerprint sensor and are thus authenticated.

A second approach consists in arranging the fingerprint sensor on a module coupled with the chip card reader by a detachable plug connection. In this approach, in order to prevent the characteristic data set provided by the fingerprint sensor from being spied out in the environment of the plug connection, this characteristic data set is not transmitted directly, but in an encoded form. To this end, the module is provided with a SAM card reader and an internal processor. Using such an embodiment of the security system,

communication between a local data processing apparatus and a network or the like may also be controlled with a maximum degree of security.

Further features and advantages of the invention will be obvious from the following description and from the drawings to which reference is made and in which:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a schematic side view of a chip card reader with a chip card inserted and the sensor module slipped on;

Figure 2 is a view of an end face of the sensor module;

Figure 3 is a top view of the sensor module, with the chip card shown cut off;

Figure 4 shows three possible embodiments for the housing of the sensor module;

Figure 5 is a schematic side view of the chip card reader and the sensor module according to a further embodiment;

Figure 6 is a view of an end face of the sensor module;

Figure 7 is a top view of the sensor module;

Figure 8 is a schematic side view of a further embodiment of the chip card reader and the sensor module; and

Figure 9 is a block diagram of the security system.

DETAILED DESCRIPTION

The security system, shown in Figure 1, for identity and authorization checking in a protected communication environment comprises a chip card reader 10 in the format of a PC card and a sensor module 12 which has a fingerprint sensor 14 and is detachably coupled to the chip card reader 10 by a plug connection. The chip card reader 10 includes an accommodation channel for a chip card 16 and, arranged in the accommodation channel, a contact field 18 for contacting the chip card 16. In the case of the embodiment shown here, the

accommodation channel for the chip card is formed between a cover plate 10a and the main body 10b of the chip card reader.

The sensor module 12 is coupled to the narrow end face of the chip card reader 10, from which the chip card 16 projects. The housing of the sensor module 12 is provided with a slot 20 for the passage of the chip card 16. The fingerprint sensor 14 is embedded in the upper main surface of the sensor module 12. The sensor module 12 has a pair of guide pins 24 which are insertable into corresponding receiving openings at the narrow end face of the chip card reader 10. A series of contact pins 26 of the sensor module 12 are adapted to be inserted into corresponding contact ports on the same end face of the chip card reader 10. Actuating members 28 for a locking means are mounted on the narrow sides of the sensor module 12; by means of the locking means the sensor module 12 is detachably locked with the chip card reader 10. Figure 3 also illustrates the contact surface 16a of the chip card 16. With the chip card 16 inserted in the chip card reader 10, the contact surface 16a ends up lying beneath the contact field 18.

Depending on how the accommodation channel for the chip card 16 is arranged in the chip card reader, the slot 20 to be seen in Figure 2 is provided in the housing of the sensor module 12, or otherwise, recesses 20a and 20b are provided at the underside and at the upper side, respectively, of the sensor module 12, as illustrated in Figure 4.

In the embodiment illustrated in Figure 5, the sensor module 12 has formed thereon a housing block with a ramp-shaped supporting surface in which the fingerprint sensor 14 is embedded. In addition, the sensor module 12 is configured for receiving and reading a so-called SAM card or SIM card 32. The card in question is a known security and authentication module.

A further component of the sensor module 12 is an interface for the connection to a communication system; in the embodiment shown, this is a network media adapter to which a network cable 34 is connected by means of a plug connector 36.

Figure 8 shows an embodiment of the chip card reader with an accommodation channel for the chip card which is formed between a bottom plate and the main body of the chip card reader.

The concept underlying the security system will now be explained with reference to the block diagram in Figure 9.

The security system comprised of the chip card reader 10 with chip card 16, on the one hand, and the sensor module 12 with the fingerprint sensor 14 and the SAM card 32, on the other hand, is fitted between a data processing apparatus (PC) referred to as host and a network connection. The chip card reader 10, just like the sensor module 12, is provided with a separate local bus. The two bus systems are coupled with each other via the plug connection between the chip card reader 10 and the sensor module 12. The chip card reader 10 includes an internal processor 40 which assumes the functions of authentication, identification, cryptographic coding, and signature. On the host side the chip card reader 10 is equipped with a suitable interface 42, more particularly a PCMCIA interface. The chip card reader 10 further includes a storage 44 for secured data in flash technology and a time stamping unit 46 which may include a radio-controlled clock module. The chip card 16 is designed as a so-called smart card and has processor and storage circuits of its own. In particular, personal keys and code words for the purpose of identity and authorization checking are stored in the chip card 16. All of the above-mentioned components of the chip card reader 10 are coupled to its internal local bus.

The sensor module 12 likewise comprises an internal processor 50, the task of which consists, above all, in the analysis of the fingerprint data provided by the sensor 14 for the purpose of identification. The SAM card is read out via a contact unit 52. The SAM card has characteristic fingerprint data of the authorized user stored thereon. The communication interface of the sensor module 12 includes an interface controller 54 and a network media adapter 56, to which the network cable 34 is connected.

In addition to the characteristic fingerprint data of the authorized user the SAM card includes data and structures for encoding such data, which is then transferred to the chip card reader 10 in an encoded form for evaluation.

An encoded transmission of the fingerprint data can be done without if the fingerprint sensor and the chip card reader are integrated with each other, so that it is not possible to intercept the data from the fingerprint sensor. In the case of this alternative embodiment, the communication interface (network media adapter) is integrated in the system as well.